IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application:	:	Group Art Unit: 2136
James P. Goddard	:	Examiner: Daniel L. Hoang
Serial No.: 10/690,017	:	IBM Corporation
Filed: 10/21/2003	:	Intellectual Property Law
Confirmation No.: 4833	:	Department SHBC/040-3
Title: SYSTEM, METHOD AND PROGRAM	:	1701 North Street
PRODUCT TO DETERMINE SECURITY	:	Endicott, NY 13760
RISK OF AN APPLICATION	:	

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

THIRD APPEAL BRIEF

I. REAL PARTY IN INTEREST

International Business Machines Corporation is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1, 3, 7-10, 12, 15, 19-20 and 25-37 are pending, Twice Rejected and Appealed.

Claims 2, 4-6, 11, 13-14, 16-18 and 21-24 were previously canceled.

IV. STATUS OF AMENDMENTS

The (first) Final Rejection was mailed on April 19, 2007. Appellants filed a (first) Appeal Brief on July 10, 2007. In response to Appellants' (first) Appeal Brief of July 10, 2007, the Examiner sent a (second) Final Rejection on November 15, 2007, citing Appellants Background Information as additional prior art in combination with previously cited Goldfeder et al. Appellants filed a Second Appeal Brief on April 15, 2008 instead of responding to the (second) Final Rejection.

The Second Appeal Brief of April 15, 2008 was nonCompliant, so Appellants filed a Second Corrected Appeal Brief on May 2, 2008. In response to Appellant's Second Corrected Appeal Brief of May 2, 2008 (referenced by the Examiner as filed on May 6, 2008), the Examiner reopened prosecution with a nonFinal Action on July 21, 2008 (which was erroneously noted as a "Final Action" on the Office Action Summary). In the nonFinal Action of July 21, 2008, the Examiner rejected all pending claims under 35 USC 103(a) based on US Patent 6,374,358 to Townsend. In a telephonic interview with Examiner Daniel Hoang on August 15, 2008, the Examiner stated that the prior rejection under 35 USC 103(a) based on US Publication 2004/0230835 by Goldfedder et al. and Applicants' Background Information was withdrawn.

With the claims twice rejected, Appellants have elected to file a Notice of Appeal and this Third Appeal Brief instead of reentering prosecution and responding directly to the Examiner to the Office Action of July 21, 2008.

No amendment was submitted in response to the Office Action of July 21, 2008 or to either, prior, Final Rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Support for each claim element is indicated in plain brackets [ ].

Claim 1 recites a computer implemented method for evaluating a security risk of an application. [Computer program implementing automated processes 200 and 300.] A determination is made whether the application is shared by different customers [Decision 308 of Figure 3. Page 8 lines 16-17. First program instructions of original claim 24.] A determination is made whether a third party can have unauthorized administrative authority to data maintained by the application. [Decisions 212 and 225 of Figure 2. Page 7 lines 1-2 and 9-11.] A determination is made whether a third party can have unauthorized read and/or write access to data maintained by the application. [Decision 217 and 224 of Figure 2. Pages 7 lines 6-9.] A numerical value or weight is assigned to each of the foregoing determinations. [Steps 310, Step 226, Step 215, Step 222. Page 7 lines 6-15. Page 8 lines 17-18] Each of the numerical values or weights corresponds to a significance of the respective determination in evaluating the security risk. [Page 2 lines 7-10 and 16-18. Second program instructions of original claim 21] The numerical values or weights are combined to evaluate the security risk. [Page 4 lines 6-10. Page 7 lines 14-15, Step 310 and Page 8 lines 17-18, Steps 204, 215, 222 and 230, Page 7 lines 6-9 and 14-15].

Claim 25 recites a computer program product for evaluating a security risk of an application. [Computer program implementing automated processes 200 and 300.] First program instructions determine whether the application is shared by different customers [Decision 308 of Figure 3. Page 8 lines 16-17. First program instructions of original claim 24.] Second program instructions determine whether a third party can have unauthorized administrative authority to data maintained by the application. [Decisions 212 and 225 of Figure 2. Page 7 lines 1-2 and 9-11.] Third program instructions determine whether a third party can have unauthorized read and/or write access to data maintained by the application. [Decision 217 and 224 of Figure 2. Pages 7 lines 6-9.] Fourth program instructions assign a numerical value or weight to each of the foregoing determinations. [Steps 310, Step 226, Step 215, Step 222. Page 7 lines 6-15. Page 8 lines 17-18] Each of the numerical values or weights corresponds to a significance of the respective determination in evaluating the security risk. [Page 2 lines 7-10 and 16-18. Second program instructions of original claim 21] Fifth program instructions combine the numerical

values or weights to evaluate the security risk. [Page 4 lines 6-10. Page 7 lines 14-15, Step 310 and Page 8 lines 17-18, Steps 204, 215, 222 and 230, Page 7 lines 6-9 and 14-15].

Claim 32 recites a computer program product for evaluating a security risk of an application. [Computer program implementing automated processes 200 and 300.] First program instructions determine whether a vulnerability in the application can be exploited by a person or program which has not been authenticated to the application or a system in which the application runs. [Decision 240 of Figure 2. Page 7 lines 15-18.] Second program instructions determine whether a third party can have unauthorized administrative authority to data maintained by the application. [Decisions 212 and 225 of Figure 2. Page 7 lines 1-2 and 9-11.] Third program instructions assign a numerical value or weight to each of the foregoing determinations. [Step 242 doubling a value assigned in step 214, 215, 222, 226 and/or 228. Page 7 lines 15-18. Step 226, Page 7 lines 9-11.] Each of the numerical values or weights correspond to a significance of the respective determination in evaluating the security risk. [Page 2 lines 7-10 and 17-18. Third determining step of original claim 22.] Fourth program instructions combine the numerical values or weights to evaluate the security risk. [Page 4 lines 6-10. Page 7 lines 14-15, Steps 240, 242 and 204, Steps 225, 226 and 230, Page 7 lines 6-9 and 14-15].

VI. Grounds of Rejection To Be Reviewed Upon Appeal

Claims 1, 3, 7-10, 12, 15, 19-20 and 25-37 were rejected under 35 USC 103(e) based on US Patent 6,374,358 to Townsend.

VII. Argument

A proper rejection under 35 USC 103 requires, at a minimum, the Examiner to cite references that disclose or suggest all the elements of the claim. See In re. Rijckaert, 28 USPQ2d

1955, 1956-57 (Fed. Cir. 1993). Otherwise, the Examiner has not made a prima facie case of obviousness.

35 USC 103(a) Rejection of Claims 1, 3, 7-10, 12, 19-20 based on Townsend

Claim 1 recites a computer implemented method for evaluating a security risk of an application. A determination is made whether the application is shared by different customers. A determination is made whether a third party can have unauthorized administrative authority to data maintained by the application. A determination is made whether a third party can have unauthorized read and/or write access to data maintained by the application. A numerical value or weight is assigned to each of the foregoing determinations. Each of the numerical values or weights corresponds to a significance of the respective determination in evaluating the security risk. The numerical values or weights are combined to evaluate the security risk.

Townsend discloses:

"The organization must also determine the types of attacks that the organization may be subject to and corresponding countermeasures that may be implemented to avert those attacks (state 105). The set T of attack types, includes but is not limited to, for example, unauthorized access to and use of confidential business information, unauthorized deletion, destruction or modification of data records, and interruption or denial of service." Townsend Column 3 lines 17-24.

"Table 1 of FIG. 3A, for example, shows identified business concerns in the left-hand column and attack types across the top. Each table entry, PHI ij, represents the probability that business concern, Ci, will result from attack Tj, determined by independent security councils of security consulting organizations or from existing data from actual business practice." Column 3 lines 51-58.

FIG. 3B lists countermeasures, i.e. policy awareness, policy compliance, corporate security awareness, unique training and account revocation.

Townsend also discloses a method of selecting a security model of an organization, based on several steps.

> "After these parameters are determined for the business of the organization, each application asset in the overall system is evaluated independently using states 125-177. For each application asset, processing begins with computation of a maximum loss factor, V, for the current application asset (state 125). For each Ci, in the set of C business concerns, there exists a corresponding Vi representing a monetary value of the loss to the organization if loss of the current application asset results in the business concern Ci. The loss estimate includes such factors as cost to respond, recover or rebuild the lost or damaged application asset or to recover from the side effects caused by compromise of the application asset, such as loss of market shore, loss of revenue from crippled manufacturing operations and loss of intellectual property revenue." Townsend Column 4 lines 40-52.

> "Next, for each of n countermeasures identified in state 105, the method determines current and recommended strength levels. Current strength level is the level of a countermeasure that the organization was employing at the time of assessment." Townsend Column 5 lines 17-20.

> "Pn is the recommended strength level for the Nth countermeasure (state 145). Function F2 is a conversion function that accepts as input, Sn, the maximum effectiveness of a particular countermeasures, and returns an ordinal value representing a recommended countermeasure strength level." Townsend Column 5 lines 61-65.

"Next, the method determines the current effectiveness level of countermeasure n in preventing attacks of all types against each of the business concerns identified for this application asset." Townsend Column 5 lines 34-37.

"Once all the countermeasures have been evaluated, the level of conformance to recommended security policies is calculated (state 170). The level of conformance of the application system at the time of assessment, or application risk, is the difference between current strength level effectiveness and recommended strength level effectiveness of the countermeasure." Townsend Column 6 line 66 to Column 7l line 5.

Townsend also disclose,

"If any of the processors in the application system serve multiple functions, such as serving both as a file transfer server and a gateway, some of the countermeasures and recommended countermeasures may need to be adjusted. Additionally, some countermeasure strengths may need to be adjusted if the size of the user population exceeds a designated threshold. Organizations with user populations over a threshold, for example, may want to initiate more formal account management procedures such a periodic mandatory password changes, formal procedures for terminated or inactive accounts, or central password administration. Another example of an exception condition possibly warranting special attention is number and value of transactions processed by the application. If, for example, the application is used to access bank account data or make large payments, the organization may want to employ added security protections such as formalized configuration management, compartmentalizing data, special audit procedures, or requiring a minimum of two people acknowledging changes to the application code." Townsend Column 7 lines 39-60.

However, Townsend does not disclose or suggest the following features of present claim 1. A determination is made whether the application is shared by different *customers*. A determination is made whether a third party can have unauthorized *administrative authority* to

data maintained by the application. These important factors of present claim 1 are used to evaluate the magnitude of a security risk, and are not taught or suggested by Townsend. Also, while Townsend assign a monetary value to loss of an application asset and assign a strength level to a countermeasure, unlike present claim 1, Townsend does not assign numerical values or weights that correspond to significance of whether the application is shared by different *customers* and whether a third party can have unauthorized *administrative authority* to data maintained by the application. In summary, Townsend is concerned with assessing the value of protecting an asset and the strength of a countermeasure. However, Townsend does not consider the foregoing factors of present claim 1 in assessing and quantifying the security risk. Therefore, Townsend fail to teach or render obvious claim 1, and the rejection under 35 USC 103(a) should be reversed.

Claims 3, 7-10, 12 and 19-20 depend on claim 1, and therefore distinguish over Townsend for the same reasons that claim 1 distinguishes thereover. Therefore, the rejection of claims 3, 7-10, 12 and 19-20 under 35 USC 103 should be reversed.

35 USC 103(a) Rejection of Claims 25-28,
based on Townsend

Independent claim 25 distinguishes over Townsend for the same reasons that claim 1 distinguishes thereover. In addition, claim 25 recites a computer program product for performing the functions. Therefore, the rejection of claim 25 under 35 USC 103 should be reversed. Claims 26-28 depend on claim 25, and therefore the rejection of claims 26-28 under 35 USC 103 should be reversed for the same reasons.

35 USC 103(a) Rejection of Claims 30-31
based on Townsend

Claims 30-31 depend on claim 25 and therefore distinguish over Townsend for the same reasons that claim 25 distinguishes thereover. Therefore, the rejection of claims 30-31 under 35 USC 103 should be reversed.

35 USC 103(a) Rejection of Claims 32-34 based on Townsend

Claim 32 recites a computer program product for evaluating a security risk of an application. First program instructions determine whether a vulnerability in the application can be exploited by a person or program which has not been authenticated to the application or a system in which the application runs. Second program instructions determine whether a third party can have unauthorized **administrative authority** to data maintained by the application. Third program instructions assign a numerical value or weight to each of the foregoing determinations. Each of the numerical values or weights corresponds to a significance of the respective determination in evaluating the security risk. Fourth program instructions combine the numerical values or weights to evaluate the security risk.

Thus, the present invention as recited in claim 32 determines if a **third party** can have unauthorized **administrative authority** to data maintained by the application, and assigns a numerical value or weight to each of the foregoing determinations. This is not taught or suggested by Townsend, as explained above. Moreover, Townsend do not disclose this determination in a computer implemented process for evaluating a security risk. Therefore, the rejection of claim 32 under 35 USC 103 should be reversed.

Claims 33-34 depend on claim 32 and therefore distinguish over Townsend for the same reasons that claim 32 distinguishes thereover. Therefore, the rejection of claims 33-34 under 35 USC 103 should be reversed.

35 USC 103(a) Rejection of Claims 36-37 based on Townsend

Claims 36-37 depend on claim 32 and therefore distinguish over Townsend for the same reasons that claim 32 distinguishes thereover. Therefore, the rejection of claims 36-37 under 35 USC 103 should be reversed.

35 USC 103(a) rejection of Claims 15, 29 and 35
Based on Townsend

Claim 15 depends on claim 1 and further recites the following. A determination is made whether there is a requirement for authentication of the application or a system in which the application runs to other systems **before connection of the application or the system in which the application runs to said other systems**. A numerical value or weight is assigned to this determination and used in evaluating the security risk. This is not taught or suggested by Townsend.

The Examiner cited the following against claim 15:

> "The set M of countermeasures may include, for example, employing a person (such as an account or security administrator to oversee security measures), implementing a technique (such as password protection, event logging, or authentication), or installing a device (such as a particular security network configuration)." Townsend Column 3 lines 24-29.

But this is not a determination whether there is a requirement for authentication of the application or a system in which the application runs to other systems **before connection of the application or the system in which the application runs to said other systems**. Claim 15 recites a determination whether there is prior authentication before a connection is made to the target application, and use of this determination to assess a security risk. (This factor reduces the security risk.) A numerical value or weight is assigned to this determination and used in evaluating the security risk. This is not taught or suggested by Townsend. Therefore, the rejection of claim 15 under 35 USC 103 should be reversed for the same reason that the rejection of claim 1 should be reversed and the additional reason explained above.

Claim 29 depends on claim 25, and further distinguishes over Townsend as does claim 15. In addition, claim 29 recites a computer program product which performs this function. Therefore, the rejection of claim 29 under 35 USC 103 should be reversed for the same reason that the rejection of claim 25 should be reversed and the additional reasons explained above.

Claim 35 depends on claim 32, and further distinguishes over Townsend as does claim 15. In addition, claim 35 recites a computer program product which performs this function. Therefore, the rejection of claim 35 under 35 USC 103 should be reversed for the same reasons that the rejection of claim 32 should be reversed and the additional reason explained above.

Based on the foregoing, the rejection under 35 USC 103 of all pending claims should be reversed.

Respectfully submitted,

Dated: 08/28/2008
Telephone: 607-429-4368
Fax No.: 607-429-4119

/Arthur J. Samodovitz/
Arthur J. Samodovitz
Reg. No. 31,297

VIII. CLAIMS APPENDIX:

1. A computer implemented method for evaluating a security risk of an application, said method comprising the steps of:

determining whether the application is shared by different customers;

determining whether a third party can have unauthorized administrative authority to data maintained by said application;

determining whether a third party can have unauthorized read and/or write access to data maintained by said application;

assigning a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the respective determination in evaluating said security risk; and

combining said numerical values or weights to evaluate said security risk.

3. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether said application is subject to industry controls for security; and

assigning a numerical value or weight to the determination whether said application is subject to industry controls for security, and using the numerical value or weight for the determination whether said application is subject to industry controls for security in evaluating said security risk.

7. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether a third party can have unauthorized read and write access to said data; and

assigning a numerical value or weight to the determination whether a third party can have unauthorized read and write access to said data, and using the numerical value or weight for the determination whether a third party can have unauthorized read and write access to said data in evaluating said security risk.

8. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and

assigning a numerical value or weight to the determination whether the vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs and using the numerical value or weight to the determination whether the vulnerability in said application can be exploited by a program or person which has not been authenticated to said application or a system in which said application runs in evaluating said security risk.

9. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether said data maintained by by said application is confidential; and wherein

the numerical value or weight assigned to the determination whether a third party can have unauthorized write access to said data is based in part on whether said data is confidential.

10. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether a customer has direct use of said application; and

assigning a numerical value or weight to the determination whether a customer has direct use of said application, and using the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk.

12. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether there is an intrusion detection system and vulnerability scanning for said application; and

assigning a numerical value or weight to the determination whether there is an intrusion detection system and vulnerability scanning for said application, and using the numerical value or weight for the determination whether there is an intrusion detection system and vulnerability scanning for said application in evaluating said security risk.

15. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems; and

assigning a numerical value or weight to the determination whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems, and using the numerical value or weight for said requirement for authentication in evaluating said security risk.

19. A computer implemented method as set forth in claim 1 further comprising the step of comparing the evaluation of said security risk to a cost savings provided by said application, and determining whether to certify said application for use based in part on said comparison.

20. A computer implemented method as set forth in claim 1 further comprising the step of comparing the evaluation of said security risk to a revenue provided by said application, and determining whether to certify said application for use based in part on said comparison.

25. A computer program product for evaluating a security risk of an application, said computer program product comprising:

a computer readable media;

first program instructions to determine whether the application is shared by different customers;

second program instructions to determine whether a third party can have unauthorized administrative authority to data maintained by said application;

third program instructions to determine whether a third party can have unauthorized read and/or write access to data maintained by said application;

fourth program instructions to assign a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the respective determination in evaluating said security risk; and

fifth program instructions to combine said numerical values or weights to evaluate said security risk; and wherein

said first, second, third, fourth and fifth program instructions are recorded on said media.

26. A computer program product as set forth in claim 25 wherein:

said third program instructions determine whether a third party can have unauthorized read and write access to said data;

said fourth program instructions assign a numerical value or weight to the determination whether a third party can have unauthorized read and write access to said data; and

said fifth program instructions also use the numerical value or weight for the determination whether a third party can have unauthorized read and write access to said data in evaluating said security risk.

27. A computer program product as set forth in claim 25 further comprising:

sixth program instructions to determine whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and

seventh program instructions to assign a numerical value or weight to the determination whether the vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and wherein

said fifth program instructions also use the numerical value or weight to the determination whether the vulnerability in said application can be exploited by a program or person which has not been authenticated to said application or a system in which said application runs to evaluate said security risk; and

said sixth and seventh program instructions are recorded on said media in functional form.

28. A computer program product as set forth in claim 25 further comprising:

sixth program instructions to determine whether a customer has direct use of said application; and

seventh program instructions to assign a numerical value or weight to the determination whether a customer has direct use of said application; and wherein

said fifth program instructions also use the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk; and

said sixth and seventh program instructions are recorded on said media.

29. A computer program product as set forth in claim 25 further comprising:

sixth program instructions to determine whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems; and

fifth program instructions to assign a numerical value or weight to the determination whether there is said requirement for authentication; and wherein

said fifth program instructions also use the numerical value or weight for said requirement for authentication in evaluating said security risk; and

said sixth and seventh program instructions are recorded on said media.

30. A computer program product as set forth in claim 25 further comprising:

sixth program instructions to compare the evaluation of said security risk to a cost savings provided by said application, and determine whether to certify said application for use based in part on said comparison; and wherein

said sixth program instructions are recorded on said media.

31. A computer program product as set forth in claim 25 further comprising:

sixth program instructions to compare the evaluation of said security risk to a revenue provided by said application, and determine whether to certify said application for use based in part on said comparison; and wherein

said sixth program instructions are recorded on said media.

32. A computer program product for evaluating a security risk of an application, said computer program product comprising:

a computer readable media;

first program instructions to determine whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs;

second program instructions to determine whether a third party can have unauthorized administrative authority to data maintained by said application;

third program instructions to assign a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the respective determination in evaluating said security risk; and

fourth program instructions to combine said numerical values or weights to evaluate said security risk; and wherein

said first, second, third and fourth program instructions are recorded on said media.

33. A computer program product as set forth in claim 32 further comprising:

fifth program instructions to determine whether a third party can have unauthorized read and/or write access to data maintained by said application; and

sixth program instructions to assign a numerical value or weight to the determination whether a third party can have unauthorized read and/or write access to data maintained by said application; and wherein

said fourth program instructions also use the numerical value or weight to the determination whether a third party can have unauthorized read and/or write access to data maintained by said application to evaluate said security risk; and

said fifth and sixth program instructions are recorded on said media in functional form.

34. A computer program product as set forth in claim 32 further comprising:

fifth program instructions to determine whether a customer has direct use of said application; and

sixth program instructions to assign a numerical value or weight to the determination whether a customer has direct use of said application; and wherein

said fourth program instructions also use the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk; and

said fifth and sixth program instructions are recorded on said media.

35. A computer program product as set forth in claim 32 further comprising:

fifth program instructions to determine whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems; and

sixth program instructions to assign a numerical value or weight to the determination whether there is said requirement for authentication of said application or said system; and wherein

said fourth program instructions also use the numerical value or weight for said requirement for authentication of said application or said system in evaluating said security risk; and

said fifth and sixth program instructions are recorded on said media.

36. A computer program product as set forth in claim 32 further comprising:

fifth program instructions to compare the evaluation of said security risk to a cost savings provided by said application, and determine whether to certify said application for use based in part on said comparison; and wherein

said fifth program instructions are recorded on said media.

37. A computer program product as set forth in claim 32 further comprising:

fifth program instructions to compare the evaluation of said security risk to a revenue provided by said application, and determine whether to certify said application for use based in part on said comparison; and wherein

said fifth program instructions are recorded on said media.

IX. Evidence Appendix

There is no evidence entered or relied upon in the appeal.

X. Related Proceedings Appendix

There are no related proceedings and therefore no copies of decisions to provide.